

Sequent Calculus in the Topos of Trees

Ranald Clouston¹ and Rajeev Goré²

¹ Department of Computer Science, Aarhus University
ranald.clouston@cs.au.dk

² Research School of Computer Science, Australian National University
rajeev.gore@anu.edu.au

Abstract. Nakano’s “later” modality, inspired by Gödel-Löb provability logic, has been applied in type systems and program logics to capture guarded recursion. Birkedal et al modelled this modality via the internal logic of the topos of trees. We show that the semantics of the propositional fragment of this logic can be given by linear converse-well-founded intuitionistic Kripke frames, so this logic is a marriage of the intuitionistic modal logic KM and the intermediate logic LC. We therefore call this logic KM_{lin} . We give a sound and cut-free complete sequent calculus for KM_{lin} via a strategy that decomposes implication into its static and irreflexive components. Our calculus provides deterministic and terminating backward proof-search, yields decidability of the logic and the coNP-completeness of its validity problem. Our calculus and decision procedure can be restricted to drop linearity and hence capture KM.

1 Introduction

Guarded recursion [10] on an infinite data structure requires that recursive calls be nested beneath constructors. For example, a stream of zeros can be defined with the self-reference guarded by the cons:

zeros = 0 : zeros

Such equations have *unique* solutions and are *productive*: they compute arbitrarily large prefixes of the infinite structure in finite time, a useful property in lazy programming.

Syntactic checks do not always play well with higher-order functions; the insight of Nakano [26] is that guarded recursion can be enforced through the *type system* via an ‘approximation modality’ inspired by Gödel-Löb provability logic [7]. We follow Appel et al [1] and call this modality *later*, and use the symbol \triangleright . The meaning of $\triangleright\tau$ is roughly ‘ τ one computation step later’. Type definitions must have their self-reference guarded by later. For example streams of integers, which we perhaps expect to be defined as $Stream \cong \mathbb{Z} \times Stream$, are instead

$$Stream \cong \mathbb{Z} \times \triangleright Stream$$

Nakano showed that versions of Curry’s fixed-point combinator \mathbf{Y} , and Turing’s fixed-point combinator likewise, can be typed by the *strong Löb axiom* (see [23])

$$(\triangleright\tau \rightarrow \tau) \rightarrow \tau \tag{1}$$

Returning to our example, \mathbf{Y} can be applied to the function

$$\lambda x. \langle 0, x \rangle : \triangleright Stream \rightarrow \mathbb{Z} \times \triangleright Stream$$

to define the stream of zeros.

Nakano’s modality was popularised by the typing discipline for intermediate and assembly languages of Appel et al [1], where for certain ‘necessary’ types a ‘Löb rule’ applies which correlates to the strong Löb axiom (1). The modality has since been applied in a wide range of ways; a non-exhaustive but representative list follows. As a type constructor, \triangleright appears in Rowe’s type system for Featherweight Java [29], the kind system of the System F extension FORK [27], and in types for functional reactive programming [21], with applications to graphical user interfaces [20]. As a logical connective, \triangleright was married to separation logic in [18], then to higher-order separation logic in [2], and to *step-indexed* logical relations for reasoning about programming languages with LSLR [12]. Thus Nakano’s modality is important in various applications in computer science.

We have so far been coy on precisely what the logic of later is, beyond positing that \triangleright is a modality obeying the strong Löb axiom. Nakano cited Gödel-Löb provability logic as inspiration, but this is a *classical* modal logic with the *weak* Löb axiom $\Box(\Box\tau \rightarrow \tau) \rightarrow \Box\tau$, whereas we desire intuitionistic implication and the stronger axiom (1). In fact there does exist a tradition of intuitionistic analogues of Gödel-Löb logic [23], of which Nakano seemed mainly unaware; we will see that logic with later can partly be understood through this tradition. In the computer science literature it has been most common to leave proof theory and search implicit and fix some concrete semantics; for example see Appel et al’s Kripke semantics of stores [1]. A more abstract and general model can be given via the internal logic of the *topos of trees* \mathcal{S} [4]. This was shown to generalise several previous models for logic with later, such as the ultrametric spaces of [5,21], and provides the basis for a rich theory of dependent types. We hence take the internal logic of \mathcal{S} as a prominent and useful model of logic with later, in which we can study proof theory and proof search.

In this paper we look at the propositional-modal core of the internal logic of \mathcal{S} . This fragment will be seen to have semantics in *linear intuitionistic Kripke frames* whose reflexive reduction is *converse-well-founded*. Linear intuitionistic frames are known to be captured by the *intermediate* logic Dummett’s LC [8]; the validity of the LC axiom in the topos of trees was first observed by Litak [22]. Intuitionistic frames with converse-well-founded reflexive reduction are captured by the intuitionistic modal logic KM, first called I^Δ [25]. Hence the internal propositional modal logic of the topos of trees is semantically exactly their combination, which we call KM_{lin} (Litak [23, Thm. 50] has subsequently confirmed this relationship at the level of Hilbert axioms also).

Our specific contribution is to give a sound and cut-free complete sequent calculus for KM_{lin} , and by restriction for KM also, supporting terminating backwards proof search and hence yielding the decidability and finite model property of these logics. Our sequent calculus also establishes the coNP-completeness of deciding validity in KM_{lin} .

To our knowledge sequent calculi for intuitionistic Gödel-Löb logics, let alone KM or KM_{lin} , have not before been investigated, but such proof systems provide a solid foundation for proving results such as decidability, complexity, and interpolation, and given an appropriate link between calculus and semantics can provide explicit, usually finite, counter-models falsifying given non-theorems.

The main technical novelty of our sequent calculus is that we leverage the fact that the intuitionistic accessibility relation is the reflexive closure of the modal relation, by decomposing implication into a static (classical) component and a dynamic ‘irreflexive implication’ \rightarrow that looks forward along the modal relation. In fact, this irreflexive implication obviates the need for \triangleright entirely, as $\triangleright\varphi$ is easily seen to be equivalent to $\top \rightarrow \varphi$. Semantically the converse of this applies also, as $\varphi \rightarrow \psi$ is semantically equivalent to $\triangleright(\varphi \rightarrow \psi)$ ³, but the \rightarrow connective is a necessary part of our calculus. We maintain \triangleright as a first-class connective in deference to the computer science applications and logic traditions from which we draw, but note that formulae of the form $\triangleright(\varphi \rightarrow \psi)$ are common in the literature - see Nakano’s $(\rightarrow E)$ rule [26], and even more directly Birkedal and Møgelberg’s \otimes constructor. We therefore suspect that treating \rightarrow as a first-class connective could be a conceptually fruitful side-benefit of our work.

2 From the Topos of Trees to Kripke Frames

In this section we outline the *topos of trees* model and its internal logic, and show that this logic can be described semantically by conditions on intuitionistic Kripke frames. Therefore after this section we discard category theory and proceed with reference to Kripke frames alone.

The topos of trees, written \mathcal{S} , is the category of presheaves on the first infinite ordinal ω (with objects $1, 2, \dots$, rather than starting at 0, in keeping with the relevant literature). Concretely an *object* A is a pair of a family of sets A_i indexed by the positive integers, and a family of *restriction functions* $r_i^A : A_{i+1} \rightarrow A_i$ indexed similarly. An *arrow* $f : A \rightarrow B$ is a family of functions $f_i : A_i \rightarrow B_i$ indexed similarly, subject to *naturality*, i.e. all squares below commute:

$$\begin{array}{ccccc} A_1 & \xleftarrow{a_1} & A_2 & \xleftarrow{a_2} & A_3 & \cdots & A_j & \xleftarrow{a_j} & A_{j+1} \\ f_1 \downarrow & & f_2 \downarrow & & f_3 \downarrow & & f_j \downarrow & & f_{j+1} \downarrow \\ B_1 & \xleftarrow{b_1} & B_2 & \xleftarrow{b_2} & B_3 & \cdots & B_j & \xleftarrow{b_j} & B_{j+1} \end{array}$$

Two \mathcal{S} -objects are of particular interest: the *terminal object* 1 has singletons as component sets and identities as restriction functions; the *subobject classifier* Ω has $\Omega_j = \{0, \dots, j\}$ and $\omega_j(k) = \min(j, k)$. We regard the positive integers as *worlds* and functions $x : 1 \rightarrow \Omega$ as *truth values* over these worlds, by considering x true at j iff $x_j = j$. Such an x is constrained by naturality to have one of three forms: $x_j = j$ for all j (*true everywhere*); $x_j = 0$ for all j (*true nowhere*); or

³ This in turn is equivalent in KM_{lin} (but is not in KM) to $\triangleright\varphi \rightarrow \triangleright\psi$ [26, Sec. 3].

given any positive integer k , x_j is k for all $j \geq k$, and is j for all $j \leq k$ (*becomes true at world k , remains true at all lesser worlds*). As such the truth values can be identified with the set $\mathbb{N} \cup \{\infty\}$, where ∞ captures ‘true everywhere’.

Formulae of the internal logic of \mathcal{S} are defined as

$$\varphi ::= p \mid \top \mid \perp \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \rightarrow \varphi \mid \varphi \twoheadrightarrow \varphi \mid \triangleright \varphi$$

where $p \in \text{Atm}$ is an atomic formula. Negation may be defined as usual as $\varphi \rightarrow \perp$. The connective \twoheadrightarrow , read as *irreflexive implication*, is not in Birkedal et al [4] but is critical to the sequent calculus of this paper; readers may view \twoheadrightarrow as a second-class connective generated and then disposed of by our proof system, or as a novel first-class connective, as they prefer.

Given a map η from propositional variables $p \in \text{Atm}$ to arrows $\eta(p) : 1 \rightarrow \Omega$, and a positive integer j , the Kripke-Joyal forcing semantics for \mathcal{S} are defined by

$$\begin{array}{ll} \eta, j \Vdash p & \text{iff } \eta(p)_j = j \\ \eta, j \Vdash \top & \text{always} \\ \eta, j \Vdash \perp & \text{never} \\ \eta, j \Vdash \varphi \wedge \psi & \text{iff } \eta, j \Vdash \varphi \text{ and } \eta, j \Vdash \psi \\ \eta, j \Vdash \varphi \vee \psi & \text{iff } \eta, j \Vdash \varphi \text{ or } \eta, j \Vdash \psi \\ \eta, j \Vdash \varphi \rightarrow \psi & \text{iff } \forall k \leq j. \eta, k \Vdash \varphi \text{ implies } \eta, k \Vdash \psi \\ \eta, j \Vdash \varphi \twoheadrightarrow \psi & \text{iff } \forall k < j. \eta, k \Vdash \varphi \text{ implies } \eta, k \Vdash \psi \\ \eta, j \Vdash \triangleright \varphi & \text{iff } \forall k < j. \eta, k \Vdash \varphi \end{array}$$

A formula φ is *valid* if $\eta, j \Vdash \varphi$ for all η, j . Note that $\varphi \twoheadrightarrow \psi$ is equivalent to $\triangleright(\varphi \rightarrow \psi)$, and $\triangleright \varphi$ is equivalent to $\top \twoheadrightarrow \varphi$. While implication \rightarrow can be seen as a conjunction of static and irreflexive components:

$$j \Vdash \varphi \rightarrow \psi \quad \text{iff} \quad (j \Vdash \varphi \text{ implies } j \Vdash \psi) \text{ and } j \Vdash \varphi \twoheadrightarrow \psi \quad (2)$$

it is not definable from the other connectives, because we have no static (that is, classical) implication. However our sequent calculus will effectively capture (2).

We now turn to Kripke frame semantics. Kripke semantics for intuitionistic modal logics are usually defined via bi-relational frames $\langle W, R_{\rightarrow}, R_{\square} \rangle$, where R_{\rightarrow} and R_{\square} are binary relations on W , with certain interaction conditions ensuring that modal formulae persist along the intuitionistic relation [32]. However for KM and KM_{lin} the intuitionistic relation is definable in terms of the box relation, and so only the latter relation need be explicitly given to define a frame:

Definition 2.1. A frame is a pair $\langle W, R \rangle$ where W is a non-empty set and R a binary relation on W . A KM-frame has R transitive and converse-well-founded, i.e. there is no infinite sequence $x_1 R x_2 R x_3 R \dots$. A KM_{lin} -frame is a KM-frame with R also connected, i.e. $\forall x, y \in W. x = y \text{ or } R(x, y) \text{ or } R(y, x)$.

Converse-well-foundedness implies irreflexivity. Also, KM- and KM_{lin} -frames may be infinite because non-well-founded chains $\dots R w_3 R w_2 R w_1$ are permitted.

Given a binary relation R , let $R^=$ be its *reflexive closure*. If $\langle W, R \rangle$ is a KM-frame then $\langle W, R^= \rangle$ is reflexive and transitive so provides frame semantics for

intuitionistic logic. In fact frames arising in this way in general satisfy only the theorems of intuitionistic logic, so KM is conservative over intuitionistic logic. In other words, the usual propositional connectives are too coarse to detect the converse well-foundedness of a frame; for that we need \triangleright and the strong Löb axiom (1). Similarly the reflexive closure of a KM_{lin} -frame is a *linear* relation and so gives semantics for the logic LC, over which KM_{lin} is conservative.

A *model* $\langle W, R, \vartheta \rangle$ consists of a frame $\langle W, R \rangle$ and a valuation $\vartheta : \text{Atm} \mapsto 2^W$ obeying **persistence**:

$$\text{if } w \in \vartheta(p) \text{ and } wRx \text{ then } x \in \vartheta(p)$$

We hence define KM- and KM_{lin} -models by the relevant frame conditions.

We can now define when a KM- or KM_{lin} -model $M = \langle W, R, \vartheta \rangle$ makes a formula true at a world $w \in W$, with obvious cases $\top, \perp, \wedge, \vee$ omitted:

$$\begin{array}{ll} M, w \Vdash p & \text{iff } w \in \vartheta(p) \\ M, w \Vdash \varphi \rightarrow \psi & \text{iff } \forall x. wR^-x \text{ and } M, x \Vdash \varphi \text{ implies } M, x \Vdash \psi \\ M, w \Vdash \varphi \twoheadrightarrow \psi & \text{iff } \forall x. wRx \text{ and } M, x \Vdash \varphi \text{ implies } M, x \Vdash \psi \\ M, w \Vdash \triangleright \varphi & \text{iff } \forall x. wRx \text{ implies } M, x \Vdash \varphi \end{array}$$

Thus \triangleright is the usual modal box. As usual for intuitionistic logic, we have a monotonicity lemma, provable by induction on the formation of φ :

Lemma 2.2 (Monotonicity). *If $M, w \Vdash \varphi$ and wRv then $M, v \Vdash \varphi$.*

Fixing a class of models (KM- or KM_{lin} -), a formula φ is *valid* if for every world w in every model M we have $M, w \Vdash \varphi$. It is easy to observe that the two semantics presented above coincide, given the right choice of frame conditions:

Theorem 2.3. *Formula φ is valid in the internal logic of \mathcal{S} iff it is KM_{lin} -valid.*

3 The Sequent Calculus SKM_{lin} for KM_{lin}

A *sequent* is an expression of the form $\Gamma \vdash \Delta$ where Γ and Δ are finite, possibly empty, sets of formulae with Γ the *antecedent* and Δ the *succedent*. We write Γ, φ for $\Gamma \cup \{\varphi\}$. Our sequents are “multiple-conclusioned” since the succedent Δ is a finite set rather than a single formula as in “single-conclusioned” sequents.

A sequent *derivation* is a finite tree of sequents where each internal node is obtained from its parents by instantiating a rule. The root of a derivation is the *end-sequent*. A sequent derivation is a *proof* if all the leaves are zero-premise rules. A rule may require extra side-conditions for its (backward) application.

The sequent calculus SKM_{lin} is shown in Fig. 1, where $\Gamma, \Delta, \Phi, \Theta$, and Σ , with superscripts and/or subscripts, are finite, possibly empty, sets of formulae.

Rules $\top R, \perp L, id, \vee L, \vee R, \wedge L, \wedge R$ are standard for a multiple-conclusioned calculus for Int [31]. Rules $\rightarrow L$ and $\rightarrow R$ can be seen as branching on a conjunction of static and an irreflexive implication: see equation (2). The occurrence of $\varphi \twoheadrightarrow \psi$ in the right premise of $\rightarrow L$ is redundant, since ψ implies $\varphi \twoheadrightarrow \psi$, but its presence makes our termination argument simpler.

$$\begin{array}{c}
\text{TR} \frac{}{\Gamma \vdash \top, \Delta} \quad \text{id} \frac{}{\Gamma, \varphi \vdash \varphi, \Delta} \quad \perp\text{L} \frac{}{\Gamma, \perp \vdash \Delta} \\
\\
\vee\text{L} \frac{\Gamma, \varphi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta} \quad \vee\text{R} \frac{\Gamma \vdash \varphi, \psi, \Delta}{\Gamma \vdash \varphi \vee \psi, \Delta} \\
\\
\wedge\text{L} \frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta} \quad \wedge\text{R} \frac{\Gamma \vdash \varphi, \Delta \quad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \varphi \wedge \psi, \Delta} \\
\\
\rightarrow\text{L} \frac{\Gamma, \varphi \rightarrow \psi \vdash \varphi, \Delta \quad \Gamma, \varphi \rightarrow \psi, \psi \vdash \Delta}{\Gamma, \varphi \rightarrow \psi \vdash \Delta} \quad \rightarrow\text{R} \frac{\Gamma, \varphi \vdash \psi, \Delta \quad \Gamma \vdash \varphi \rightarrow \psi, \Delta}{\Gamma \vdash \varphi \rightarrow \psi, \Delta} \\
\\
\text{STEP} \frac{\text{Prem}_1 \quad \dots \quad \text{Prem}_k \quad \text{Prem}_{k+1} \quad \dots \quad \text{Prem}_{k+n}}{\Sigma_l, \Theta^\triangleright, \Gamma^{\rightarrow} \vdash \Delta^{\rightarrow}, \Phi^\triangleright, \Sigma_r} \dagger \\
\\
\text{Prem}_{1 \leq i \leq k} = \Sigma_l, \Theta, \Theta^\triangleright, \Gamma^{\rightarrow}, \varphi_i \rightarrow \psi_i, \varphi_i \vdash \psi_i, \Delta_{-i}^{\rightarrow}, \Phi \\
\text{Prem}_{k+1 \leq i \leq k+n} = \Sigma_l, \Theta, \Theta^\triangleright, \Gamma^{\rightarrow}, \triangleright \phi_{i-k} \vdash \Delta^{\rightarrow}, \Phi \\
\\
\Theta^\triangleright = \triangleright \theta_1, \dots, \triangleright \theta_j \quad \Theta = \theta_1, \dots, \theta_j \\
\Gamma^{\rightarrow} = \{\alpha_1 \rightarrow \beta_1, \dots, \alpha_l \rightarrow \beta_l\} \quad \Gamma^{\rightarrow} = \{\alpha_1 \rightarrow \beta_1, \dots, \alpha_l \rightarrow \beta_l\} \\
\Delta^{\rightarrow} = \{\varphi_1 \rightarrow \psi_1, \dots, \varphi_k \rightarrow \psi_k\} \quad \Delta^{\rightarrow} = \{\varphi_1 \rightarrow \psi_1, \dots, \varphi_k \rightarrow \psi_k\} \\
\Delta_{-i}^{\rightarrow} = \Delta^{\rightarrow} \setminus \{\varphi_i \rightarrow \psi_i\} \\
\Phi^\triangleright = \triangleright \phi_1, \dots, \triangleright \phi_n \quad \Phi = \phi_1, \dots, \phi_n
\end{array}$$

where \dagger means that the conditions C0, C1 and C2 below must hold

(C0) $\Delta^{\rightarrow} \cup \Phi^\triangleright \neq \emptyset$

(C1) $\perp \notin \Sigma_l$ and $\top \notin \Sigma_r$ and $(\Sigma_l \cup \Theta^\triangleright \cup \Gamma^{\rightarrow}) \cap (\Delta^{\rightarrow} \cup \Phi^\triangleright \cup \Sigma_r) = \emptyset$

(C2) Σ_l and Σ_r each contain atomic formulae only

Explanations for the conditions:

(C0) there must be at least one \triangleright - or \rightarrow -formula in the succedent of the conclusion

(C1) none of the rules $\perp\text{L}, \top\text{R}, \text{id}$ are applicable to the conclusion

(C2) none of the rules $\vee\text{L}, \vee\text{R}, \wedge\text{L}, \wedge\text{R}, \rightarrow\text{L}, \rightarrow\text{R}$ are applicable to the conclusion

Fig. 1. Rules for sequent calculus SKM_{lin}

The rule STEP resembles Sonobe's multi-premise rule for $\rightarrow\text{R}$ in LC [30,11], but its interplay of static and dynamic connectives allows us to capture the converse-well-foundedness of our frames. The reader may like to skip forward to compare it to the rules for KM in Fig. 4, which are simpler because they do not have to deal with linearity. Condition C0 is essential for soundness; C1 and C2 are not, but ensure that the STEP rule is applicable only if no other rules are applicable (upwards), which is necessary for semantic invertibility (Lem. 3.11). Note that the formulae in Θ^\triangleright appear intact in the antecedent of every premise. This is not essential as Θ implies Θ^\triangleright , but will simplify our proof of completeness. In contrast the formulae in Φ^\triangleright do not appear in the succedent of any premise.

$$\begin{array}{c}
\frac{\frac{\frac{}{(\triangleright p \rightarrow p) \rightarrow p, \triangleright p \rightarrow p, \triangleright p \vdash p} \text{mp}}{(\triangleright p \rightarrow p) \rightarrow p, \triangleright p \rightarrow p, \triangleright p \vdash p} \text{STEP} \quad \frac{\frac{}{(\triangleright p \rightarrow p) \rightarrow p, \triangleright p \rightarrow p, p \vdash p} \text{id}}{(\triangleright p \rightarrow p) \rightarrow p, \triangleright p \rightarrow p, p \vdash p} \text{STEP}}{\frac{(\triangleright p \rightarrow p) \rightarrow p, \triangleright p \rightarrow p, p \vdash p}{\vdash (\triangleright p \rightarrow p) \rightarrow p} \text{STEP}} \rightarrow L \\
\\
\frac{\frac{\frac{}{\triangleright p \rightarrow p, \triangleright p \vdash p} \text{mp}}{\triangleright p \rightarrow p, \triangleright p \vdash p} \text{STEP} \quad \frac{\frac{}{\triangleright p \rightarrow p, p \vdash p} \text{id}}{\triangleright p \rightarrow p, p \vdash p} \text{STEP}}{\frac{\triangleright p \rightarrow p, p \vdash p}{\vdash (\triangleright p \rightarrow p) \rightarrow p} \text{STEP}} \rightarrow L \\
\frac{\vdash (\triangleright p \rightarrow p) \rightarrow p \quad \vdash (\triangleright p \rightarrow p) \rightarrow p}{\vdash (\triangleright p \rightarrow p) \rightarrow p} \rightarrow R
\end{array}$$

Fig. 2. SKM_{lin} proof of the strong Löb axiom

$$\begin{array}{c}
\frac{\frac{}{p \rightarrow q, p, q \vdash p, q} \text{id}}{p \rightarrow q, p \vdash q, q \rightarrow p} \text{id} \quad \frac{\frac{\frac{}{p \rightarrow q, p, q \rightarrow p, q \vdash p} \text{id}}{p \rightarrow q, p \vdash q, q \rightarrow p} \text{STEP}}{p \rightarrow q, p \vdash q, q \rightarrow p} \text{STEP} \quad \frac{\text{Symmetric to left}}{q \rightarrow p, q \vdash p, p \rightarrow q} \text{STEP}}{\vdash p \rightarrow q, q \rightarrow p} \rightarrow R \\
\\
\frac{\frac{\frac{}{p, q \vdash q, p} \text{id}}{p \vdash q, q \rightarrow p} \text{id} \quad \frac{\frac{\frac{}{p, q \rightarrow p, q \vdash p} \text{id}}{p \vdash q, q \rightarrow p} \text{STEP}}{p \vdash q, q \rightarrow p} \text{STEP} \quad \frac{\frac{\frac{}{q, p \rightarrow q, p \vdash q} \text{id}}{q \vdash p, p \rightarrow q} \text{STEP}}{q \vdash p, p \rightarrow q} \text{STEP} \quad \vdash p \rightarrow q, q \rightarrow p}{\vdash p \rightarrow q, q \rightarrow p} \rightarrow R \\
\frac{\vdash p \rightarrow q, q \rightarrow p}{\vdash p \rightarrow q \vee q \rightarrow p} \vee R
\end{array}$$

Fig. 3. SKM_{lin} proof of the LC axiom

Also, the formulae in Σ_r do not appear in the succedent of any premise. So STEP contains two aspects of weakening, but C2 ensures this is not done prematurely.

Figs. 2 and 3 give example proofs, using the following derived rule:

Lemma 3.1. *The Modus Ponens rules mp is derivable in SKM_{lin} as follows:*

Proof.

$$\frac{\frac{\frac{}{\Gamma, \varphi, \varphi \rightarrow \psi \vdash \varphi, \psi} \text{id}}{\Gamma, \varphi, \varphi \rightarrow \psi \vdash \varphi, \psi} \text{id} \quad \frac{\frac{}{\Gamma, \varphi, \varphi \rightarrow \psi, \psi \vdash \psi} \text{id}}{\Gamma, \varphi, \varphi \rightarrow \psi \vdash \psi} \text{id}}{\Gamma, \varphi, \varphi \rightarrow \psi \vdash \psi} \rightarrow L$$

3.1 Soundness of SKM_{lin}

Given a world w in some model M , and finite sets Γ and Δ of formulae, we write $w \Vdash \Gamma$ if every formula in Γ is true at w in model M and write $w \nVdash \Delta$ if every formula in Δ is not true at w in model M .

A sequent $\Gamma \vdash \Delta$ is **refutable** if there exists a model M and a world w in that model such that $w \Vdash \Gamma$ and $w \nVdash \Delta$. A sequent is **valid** if it is not refutable. A rule is **sound** if some premise is refutable whenever the conclusion is refutable.

A rule is **semantically invertible** if the conclusion is refutable whenever some premise is refutable. Given a model M and a formula φ , a world w is a **refuter** for φ if $M, w \not\models \varphi$. It is a **last refuter** for φ if in addition $M, w \Vdash \triangleright \varphi$. An **eventuality** is a formula of the form $\varphi \rightarrow \psi$ or $\triangleright \varphi$ in the succedent of the conclusion of an application of the rule STEP.

Lemma 3.2. *In every model, every formula φ with a refuter has a last refuter.*

Proof. Suppose φ has refuter w in model M , i.e. $M, w \not\models \varphi$. If all R -successors v of w have $v \Vdash \varphi$ then $w \Vdash \triangleright \varphi$, and so w is the last refuter we seek. Else pick any successor v such that $M, v \not\models \varphi$ and repeat the argument replacing w with v . By converse well-foundedness this can only be done finitely often before reaching a world with no R -successors, which vacuously satisfies $\triangleright \varphi$.

Theorem 3.3 (Soundness). *If $\vdash \varphi$ is SKM_{lin} -derivable then φ is KM_{lin} -valid.*

Proof. We consider only the non-standard rules.

→R: Suppose the conclusion $\Gamma \vdash \varphi \rightarrow \psi, \Delta$ is refutable at w in model M . Thus some R -successor v of w refutes $\varphi \rightarrow \psi$ via $M, v \Vdash \varphi$ and $M, v \not\models \psi$. If $v = w$ then w refutes the left premise $\Gamma, \varphi \vdash \psi, \Delta$. Else wRv and $M, w \not\models \varphi \rightarrow \psi$, so w refutes the right premise $\Gamma \vdash \varphi \rightarrow \psi, \Delta$.

→L: Suppose the conclusion $\Gamma, \varphi \rightarrow \psi \vdash \Delta$ is refuted at w . Hence $w \Vdash \Gamma$ and $w \Vdash \varphi \rightarrow \psi$ and $w \not\models \Delta$. Thus $w \Vdash \varphi \rightarrow \psi$. If $w \Vdash \psi$ then w refutes the right premise $\Gamma, \varphi \rightarrow \psi, \psi \vdash \Delta$. Else $w \not\models \psi$ and so we must have $w \not\models \varphi$ since we already know that $w \Vdash \varphi \rightarrow \psi$. Thus w refutes the left premise $\Gamma, \varphi \rightarrow \psi \vdash \Delta$.

STEP: Assume that $\Sigma_l, \Theta^\triangleright, \Gamma^\rightarrow \vdash \Delta^\rightarrow, \Phi^\triangleright, \Sigma_r$ is refutable. That is, there is some model M and some world w such that $M, w \Vdash \Sigma_l$ and $M, w \Vdash \Theta^\triangleright$ and $M, w \Vdash \Gamma^\rightarrow$ but $M, w \not\models \Delta^\rightarrow$ and $M, w \not\models \Phi^\triangleright$ and $M, w \not\models \Sigma_r$.

Thus each $\triangleright \phi_i \in \Phi^\triangleright$ and each $\varphi_i \rightarrow \psi_i \in \Delta^\rightarrow$ has a last refuter, which may be w itself. But then, each $\phi_i \in \Phi$ and each $\varphi_i \rightarrow \psi_i \in \Delta^\rightarrow$, has a last refuter which is a strict successor of w . From this set of strict successors of w , choose the refuter v that is closest to w in the linear order.

Since wRv , we must have $M, v \Vdash \Sigma_l$ and $M, v \Vdash \Theta$ and $M, v \Vdash \Theta^\triangleright$ and $M, v \Vdash \Gamma^\rightarrow$, giving that $M, v \Vdash \Sigma_l, \Theta, \Theta^\triangleright, \Gamma^\rightarrow$.

If v is the last refuter for some $\varphi_i \rightarrow \psi_i \in \Delta^\rightarrow$, we must have $M, v \Vdash \varphi_i$ and $M, v \not\models \psi_i$ and $M, v \Vdash \varphi_i \rightarrow \psi_i$. We must also have $M, v \not\models \Phi$ since the last refuter for each $\phi_i \in \Phi$ cannot strictly precede v , by our choice of v . For the same reason, we must have $M, v \not\models \varphi_j \rightarrow \psi_j$ for every $1 \leq j \neq i \leq k$, giving $M, v \not\models \Delta^\rightarrow_i$. Thus v refutes the i^{th} premise $\text{Prem}_i = \Sigma_l, \Gamma^\rightarrow, \Theta, \Theta^\triangleright, \varphi_i \rightarrow \psi_i, \varphi_i \vdash \psi_i, \Delta^\rightarrow_i, \Phi$.

If v is the last refuter for some $\phi_i \in \Phi$, we must have both $M, v \not\models \phi_i$ and $M, v \Vdash \triangleright \phi_i$. Since v is the closest last refuter to w in the linear order, the last refuters for the other formulae in Φ cannot strictly precede v . Hence for each $1 \leq j \neq i \leq n$, we must have $M, v \not\models \phi_j$ for each $\phi_j \in \Phi$, hence $M, v \not\models \Phi$. Moreover, for the same reason, we must have $M, v \not\models \varphi_j \rightarrow \psi_j$, where $1 \leq j \leq k$, for each $\varphi_j \rightarrow \psi_j \in \Delta^\rightarrow$, hence $M, v \not\models \Delta^\rightarrow$. That is, v refutes the $(k+i)$ -th premise $\text{Prem}_{k+i} = \Sigma_l, \Theta, \Theta^\triangleright, \Gamma^\rightarrow, \triangleright \phi_i \vdash \Delta^\rightarrow, \Phi$.

3.2 Terminating backward proof search

In this section we describe how to systematically find derivations using backward proof search. To this end, we divide the rules into three sets as follows:

Termination Rules: the rules id , $\perp L$, $\top R$

Static Rules: the rules $\rightarrow L$, $\rightarrow R$, $\vee L$, $\vee R$, $\wedge L$, $\wedge R$

Transitional Rule: STEP.

The proof search strategy below starts at the leaf (end-sequent) $\Gamma_0 \vdash \Delta_0$:

while some rule is applicable to a leaf sequent **do**
 stop: apply any applicable termination rule to that leaf
 saturate: else apply any applicable static rule to that leaf
 transition: else apply the transitional rule to that leaf

The phase where only static rules are applied is called the **saturation** phase. The only non-determinism in our procedure is the choice of static rule when many static rules are applicable, but as we shall see later, any choice suffices. Note that conditions C1 and C2 actually force STEP to have lowest priority.

Let $sf(\varphi)$ be the set of subformulae of φ , including φ itself and let m be the length of φ . Let $cl(\varphi) = sf(\varphi) \cup \{\psi_1 \multimap \psi_2 \mid \psi_1 \rightarrow \psi_2 \in sf(\varphi)\}$.

Proposition 3.4. *The (backward) saturation phase terminates for any sequent.*

Proof. Each rule either: removes a connective; or removes a formula completely; or replaces a formula $\varphi \rightarrow \psi$ with $\varphi \multimap \psi$ to which no static rule can be applied.

Given our strategy (and condition C1), we know that the conclusion of the STEP rule will never be an instance of id , hence $\varphi \multimap \psi$ or $\triangleright \varphi$ is only an eventuality when an occurrence of it does not already appear in the antecedent of the conclusion of the STEP rule in question.

Proposition 3.5. *For all rules, the formulae in the premise succedents are subformulae of formulae in the conclusion, or are \rightarrow -formulae created from \multimap -formulae in the conclusion succedent: we never create new eventualities upwards.*

Proposition 3.6. *Any application of the rule STEP has strictly fewer eventualities in each premise, than in its conclusion.*

Proof. For each premise, an eventuality $\triangleright \varphi$ crosses from the succedent of the conclusion to the antecedent of that premise and appears in all higher antecedents, or an eventuality $\varphi \multimap \psi$ from the succedent of the conclusion turns into $\varphi \rightarrow \psi$ in the antecedent of the premise and this $\varphi \rightarrow \psi$ turns back into $\varphi \multimap \psi$ via saturation, meaning that the eventuality ($\triangleright \varphi$ or $\varphi \multimap \psi$) cannot reappear in the succedent of some higher *saturated* sequent without creating an instance of id .

Theorem 3.7. *Backward proof search terminates.*

Proof. By Prop. 3.4 each saturation phase terminates, so the only way a branch can be infinite is via an infinite number of applications of the STEP rule. But by Prop. 3.6 each such application reduces the number of eventualities of the branch, and by Prop. 3.5, no rule creates new eventualities. Thus we must eventually reach a saturated sequent to which no rule is applicable, or reach an instance of a termination rule. Either way, proof search terminates.

Proposition 3.8. *Given an end-sequent $\Gamma_0 \vdash \Delta_0$, the maximum number of different eventualities is the sum of the lengths of the formula in $\Gamma_0 \cup \Delta_0$.*

Proof. Each eventuality $\triangleright\varphi$ is a subformula of the end-sequent, and each eventuality $\varphi \twoheadrightarrow \psi$ is created from a subformula $\varphi \rightarrow \psi$ which is also a subformula of the end-sequent or is a subformula of the end-sequent.

Corollary 3.9. *Any branch of our proof-search procedure for end-sequent $\Gamma_0 \vdash \Delta_0$ contains at most l applications of the STEP rule, where l is the sum of the lengths of the formulae in $\Gamma_0 \cup \Delta_0$.*

3.3 Cut-free Completeness Without Backtracking

The rules of our sequent calculus, when used according to conditions C0, C1, and C2, can be shown to preserve validity upwards as follows.

Lemma 3.10 (Semantic Invertibility). *All static rules are semantically invertible: if some premise is refutable then so is the conclusion.*

Proof. Again, we consider only the non-standard rules.

- \rightarrow R: Suppose the right premise $\Gamma \vdash \varphi \twoheadrightarrow \psi, \Delta$ is refuted at w . Then so is the conclusion $\Gamma \vdash \varphi \rightarrow \psi, \Delta$ since $\varphi \rightarrow \psi$ implies $\varphi \twoheadrightarrow \psi$.
Suppose that the left premise $\Gamma, \varphi \vdash \psi, \Delta$ is refutable at w . Then the conclusion is also refutable at w since $w \Vdash \Delta$ and $w \Vdash \varphi \rightarrow \psi$.
- \rightarrow L: Suppose the right premise $\Gamma, \varphi \twoheadrightarrow \psi, \psi \vdash \Delta$ is refuted by w . Then so is the conclusion $\Gamma, \varphi \rightarrow \psi \vdash \Delta$ since ψ implies $\varphi \rightarrow \psi$. Suppose the left premise $\Gamma, \varphi \twoheadrightarrow \psi \vdash \varphi, \Delta$ is refuted by w . Since $w \Vdash \varphi$ and $w \Vdash \varphi \twoheadrightarrow \psi$, we must have $w \Vdash \varphi \rightarrow \psi$. But $w \Vdash \Delta$, hence it refutes the conclusion.

For a given conclusion instance of the STEP rule, we have already seen that conditions C0, C1 and C2 guarantee that there is at least one eventuality in the succedent, that no termination rule is applicable, that the conclusion is saturated, and that no eventuality in the succedent of the conclusion is ignored.

Lemma 3.11. *The rule STEP (with C0, C1 and C2) is semantically invertible.*

Proof. Suppose some premise is refutable. That is,

1. for some $1 \leq i \leq k$ there exists a model $M_1 = \langle W_1, R_1, \vartheta_1 \rangle$ and $w_1 \in W_1$ such that $M_1, w_1 \Vdash \Sigma_l, \Theta, \Theta^\triangleright, \Gamma^\rightarrow, \varphi_i \twoheadrightarrow \psi_i, \varphi_i$ and $M_1, w_1 \Vdash \psi_i, \Delta_{-i}^\rightarrow, \Phi$; or

2. for some $k + 1 \leq i \leq k + n$ there exists a model $M_2 = \langle W_2, R_2, \vartheta_2 \rangle$ and $w_2 \in W_2$ such that $M_2, w_2 \Vdash \Sigma_l, \Theta, \Theta^\triangleright, \Gamma^\rightarrow, \triangleright \phi_{i-k}$ and $M_2, w_2 \not\Vdash \Delta^\rightarrow, \Phi$.

$1 \leq i \leq k$: We must show there is some model M containing a world w_0 such that $M, w_0 \Vdash \Sigma_l, \Theta^\triangleright, \Gamma^\rightarrow$ and $M, w_0 \not\Vdash \Delta^\rightarrow, \Phi^\triangleright, \Sigma_r$. We do this by taking the submodel generated by w_1 , adding an extra world w_0 as a predecessor of w_1 , letting w_0 reach every world reachable from w_1 , and setting every member of Σ_l to be true at w_0 .

We formally define M by: $W = \{w \in W_1 \mid w_1 R_1 w\} \cup \{w_0, w_1\}$; $R = \{(v, w) \in R_1 \mid v \in W, w \in W\} \cup \{(w_0, w) \mid w \in W \setminus \{w_0\}\}$; for every atomic formula p and for every $w \in W \setminus \{w_0\}$, let $w \in \vartheta(p)$ iff $w \in \vartheta_1(p)$ and put $w_0 \in \vartheta(p)$ iff $p \in \Sigma_l$.

By simultaneous induction on the size of any formula ξ , it follows that for every world $w \neq w_0$ in W , we have $M_1, w \Vdash \xi$ iff $M, w \Vdash \xi$.

We have $M, w_0 \not\Vdash \Sigma_r$ by definition (since its intersection with Σ_l is empty). We have $M, w_0 \Vdash \Theta^\triangleright$ since $M_1, w_1 \Vdash \Theta$ implies $M, w_1 \Vdash \Theta$, and we know that $w_0 R w_1$. Similarly, we have $M, w_0 \Vdash \Gamma^\rightarrow$ since $w_0 R w_1$ and $M_1, w_1 \Vdash \Gamma^\rightarrow$. Since $M_1, w_1 \Vdash \varphi_i$ and $M_1, w_1 \not\Vdash \psi_i$, we must have $M, w_0 \not\Vdash \varphi_i \rightarrow \psi_i$ as desired. Together with $M_1, w_1 \not\Vdash \Delta^\rightarrow_i$, we have $M, w_0 \not\Vdash \Delta^\rightarrow$. Finally, since $M_1, w_1 \not\Vdash \Phi$, we must have $M, w_0 \not\Vdash \Phi^\triangleright$. Collecting everything together, we have $M, w_0 \Vdash \Sigma_l, \Theta^\triangleright, \Gamma^\rightarrow$ and $M, w_0 \not\Vdash \Delta^\rightarrow, \Phi^\triangleright, \Sigma_r$ as desired.

The case $k + 1 \leq i \leq k + n$ follows similarly.

Theorem 3.12. *If the sequent $\vdash \varphi_0$ is not derivable using the rules of Fig. 1 according to our proof-search strategy then φ_0 is not KM_{lin} -valid.*

Proof. Suppose $\vdash \varphi_0$ is not derivable using our systematic backward proof search procedure. Thus our procedure gives a finite tree with at least one leaf $\Sigma_l, \Gamma^\rightarrow, \Theta^\triangleright \vdash \Sigma_r$ obeying both C1 and C2 to which no rules are applicable.

Construct $M_0 = \langle W_0, R_0, \vartheta_0 \rangle$ as follows: let $W_0 = \{w_0\}$; let $R_0 = \emptyset$; and $w_0 \in \vartheta_0(p)$ iff $p \in \Sigma_l$. Clearly, we have $M_0, w_0 \Vdash \Sigma_l$ by definition. Also, $M_0, w_0 \not\Vdash \Sigma_r$ since its intersection with Σ_l is empty by C1. Every formula $\alpha \rightarrow \beta \in \Gamma^\rightarrow$ and $\triangleright \theta \in \Theta^\triangleright$ is vacuously true at w_0 in M_0 since w_0 has no strict successors. Thus the leaf sequent $\Sigma_l, \Gamma^\rightarrow, \Theta^\triangleright \vdash \Sigma_r$ is refuted by w_0 in model M_0 . The Invertibility Lemmas 3.10 and 3.11 now imply that $\vdash \varphi_0$ is refutable in some KM_{lin} -model.

Corollary 3.13 (Completeness). *If φ is KM_{lin} -valid then $\vdash \varphi$ is SKM_{lin} -derivable.*

Cor. 3.13 guarantees that any sound rule can be added to our calculus without increasing the set of provable end-sequents, including both forms of cut below:

$$\frac{\Gamma \vdash \varphi, \Delta \quad \Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta} \quad \frac{\Gamma, \vdash \varphi, \Delta \quad \Gamma', \varphi \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

Since all static rules are semantically invertible, any order of rule applications for saturation suffices. Since all rules are invertible we never need backtracking. That is, our strategy straightforwardly yields a *decision procedure*. It also tells us that KM_{lin} , like its parent logics KM and LC, enjoys the finite model property:

Theorem 3.14. *If φ is not KM_{lin} -valid then it is refutable in a rooted (finite) KM_{lin} -model of length at most $l + 1$ where l is the length of φ .*

Proof. Suppose that φ is not valid: that is, φ is refuted by some world in some KM_{lin} model. By soundness Thm. 3.3 $\vdash \varphi$ is not derivable using our proof-search strategy. In particular, in any branch, there can be at most l applications of the rule STEP by Cor. 3.9. From such a branch, completeness Thm. 3.12 allows us to construct a model M and a world w which refutes φ . But the model M we construct in the completeness proof is a rooted (finite) KM_{lin} -model with at most $l + 1$ worlds since the only rule that creates new worlds is the (transitional) STEP rule and there are at most l such rule applications in any branch.

Corollary 3.15. *KM_{lin} has the finite model property.*

3.4 Complexity

We first embed classical propositional logic into KM_{lin} .

Lemma 3.16. *If φ is a formula built out of atomic formulae, \top and \perp using only the connectives $\wedge, \vee, \rightarrow$, and the sequent $\vdash (\varphi \rightarrow \perp) \rightarrow \perp$ is derivable, then φ is a tautology of classical propositional logic.*

Proof. Any derivation in our systematic proof search procedure ends as:

$$\frac{\frac{\varphi \rightarrow \perp \vdash \varphi, \perp \quad \dots}{\varphi \rightarrow \perp \vdash \perp} \rightarrow L \quad \dots}{\vdash (\varphi \rightarrow \perp) \rightarrow \perp} \rightarrow R$$

Thus, the sequent $\varphi \rightarrow \perp \vdash \varphi, \perp$ is derivable.

Soundness Thm. 3.3 then implies that this sequent is valid on all models. In particular, it is valid on the class of single-pointed models $M = \langle W, R, \vartheta \rangle$ where $W = \{w_0\}$ and $R = \emptyset$. The formula $\varphi \rightarrow \perp$ is true at w_0 vacuously since w_0 has no R -successor. The formula \perp is not true in any model, including this one, hence $M, w_0 \not\models \perp$. Thus $M, w_0 \models \varphi$. That is, φ itself is valid on all single-pointed models. But such a model is just a valuation of classical propositional logic.

Lemma 3.17. *If φ is a formula built out of atomic formulae, \top and \perp using only the connectives $\wedge, \vee, \rightarrow$, and the sequent $\vdash (\varphi \rightarrow \perp) \rightarrow \perp$ is not derivable, then φ is not a tautology of classical propositional logic.*

Proof. Suppose $\vdash (\varphi \rightarrow \perp) \rightarrow \perp$ is not derivable. Then, by Thm. 3.12, $(\varphi \rightarrow \perp) \rightarrow \perp$ is not KM_{lin} -valid. Thus, there is a finite linear model $M = \langle W, R, \vartheta \rangle$ with root world $w_0 \in W$ such that $M, w_0 \not\models (\varphi \rightarrow \perp) \rightarrow \perp$. Thus there is a world v such that $w_0 R v$ and $M, v \models \varphi \rightarrow \perp$, which implies that every R -successor of v , including a world u (say) with no R -successors, makes φ false. But such a final world u is just a valuation of classical propositional logic, thus there is a model of classical propositional logic which makes φ false. That is, φ is not a tautology of classical propositional logic.

Lemma 3.18. *There is a non-deterministic algorithm to test the refutability (non-validity) of the sequent $\vdash \varphi$ in time polynomial in the length of φ .*

Proof. Let l be the length of φ , and recall the definitions of $sf(\varphi)$ and $cl(\varphi)$ given earlier. The number of formulae in $cl(\varphi)$ is at most $2l$ and the size of each sequent our calculus builds is bounded by $4l^2$, since each formula of length at most l could appear in the antecedent or the succedent or both.

Let $\Gamma_1 \vdash \Delta_1, \dots, \Gamma_k \vdash \Delta_k$ be a sequence of length $k = l^2$ of sequents, where each sequent is built out of formulae from $cl(\varphi)$. Check whether this sequence forms a branch of legal rule applications, none of which is the rule *id*, and check whether no rule is applicable to the sequent $\Gamma_k \vdash \Delta_k$. If so, then the sequent $\vdash \varphi$ is refutable (non-valid).

It remains to show that this (non-deterministic) algorithm requires time which is polynomial in the length l of φ .

Every saturation phase is of length at most l since each rule removes a connective. In any branch, there can be at most l applications of the rule STEP since each eventuality which is principal in such a rule application moves into the antecedent of the appropriate premise and hence cannot reappear without leading to an instance of *id*. Thus every branch in any putative derivation of $\vdash \varphi$ is of length at most $k = l^2$. Since each sequent is of length at most $4l^2$, our procedure requires at most $4l^4$ operations. That is, it can be done in time polynomial in the length of the given end-sequent.

Corollary 3.19. *The validity problem for KM_{lin} is coNP-complete.*

Proof. By Lem. 3.16 we can faithfully embed the validity problem for classical propositional logic into KM_{lin} , hence it is at least as hard as checking validity in classical propositional logic (coNP). By Lem. 3.18, we can non-deterministically check non-validity of a given formula in time at most polynomial in its size.

4 Terminating Proof Search for KM

This section turns to logic KM, for which models need not be linear. One might expect that KM, which is conservative over Int, would require single-conclusioned sequents only, but KM-theorems such as the axiom $\triangleright \varphi \rightarrow (\psi \vee (\psi \rightarrow \varphi))$ (see Litak [23]) seem to require multiple conclusions. As such our calculus will resemble that for KM_{lin} . The static rules will be those of KM_{lin} , but the transitional rule STEP of KM_{lin} is now replaced by rules $\rightarrow R$ and $\triangleright R$ as shown in Fig. 4.

The backward proof-search strategy is the same as that of Sec. 3.2, except the transitional rule applications now reads as below:

transition: else choose a \rightarrow - or \triangleright -formula from the succedent and apply $\rightarrow R$ or $\triangleright R$, backtracking over these choices until a derivation is found or all choices of principal formula have been exhausted.

So if the given sequent is $\vdash \Delta^{\rightarrow}, \Phi^{\triangleright}, \Sigma_r$ and Δ^{\rightarrow} contains m formulae and Φ^{\triangleright} contains n formulae, then in the worst case we must explore m premise instances of $\rightarrow R$ and n premise instances of $\triangleright R$.

$$\rightarrow R \frac{\Sigma_l, \Theta, \Theta^\triangleright, \Gamma^{\rightarrow}, \varphi \rightarrow \psi, \varphi \vdash \psi}{\Sigma_l, \Theta^\triangleright, \Gamma^{\rightarrow} \vdash \varphi \rightarrow \psi, \Delta^{\rightarrow}, \Phi^\triangleright, \Sigma_r} \ddagger \quad \triangleright R \frac{\Sigma_l, \Theta, \Theta^\triangleright, \Gamma^{\rightarrow}, \triangleright \psi \vdash \psi}{\Sigma_l, \Theta^\triangleright, \Gamma^{\rightarrow} \vdash \triangleright \psi, \Delta^{\rightarrow}, \Phi^\triangleright, \Sigma_r} \ddagger$$

where \ddagger means that the following conditions hold:

(C1): $\perp \notin \Sigma_l$ and $\top \notin \Sigma_r$ and the conclusion is not an instance of *id*

(C2): Σ_l and Σ_r contain only atomic formulae (*i.e.* the conclusion is saturated)

Fig. 4. Transitional rules for logic KM

Theorem 4.1. *The rules $\rightarrow R$ and $\triangleright R$ are sound for the logic KM.*

Proof. Suppose the conclusion of rule $\rightarrow R$ is refutable at world w in some model M . Thus there is a strict R -successor v of w which is a last refuter for $\varphi \rightarrow \psi$: that is, $M, v \Vdash \varphi$ and $M, v \nVdash \psi$ and $M, v \Vdash \varphi \rightarrow \psi$. The other formulae from the antecedent of the conclusion are also true at v by truth-persistence, and for every \rightarrow -formula true at w , we also have its \rightarrow -version true at v , and likewise for \triangleright -formulae. The proof for the $\triangleright R$ rule is similar.

Termination follows using the same argument as for SKM_{lin} . However the new rules are not semantically invertible, since we have to choose a particular \rightarrow - or \triangleright -formula from the succedent of the conclusion and discard all others when moving to the premise, yet a different choice may have given a derivation of the conclusion. Thus these rules require the backtracking which is built into the new **transition** part of our proof search strategy.

Lemma 4.2. *If a sequent s obeys the \ddagger conditions and every premise instance obtained by applying the rules $\rightarrow R$ and $\triangleright R$ backwards to s is not derivable, then the sequent s is refutable.*

Proof. We proceed by induction on the maximum number k of applications of the transitional rules in any branch of backward proof search for s .

Base case $k = 0$: if s obeys the \ddagger conditions but contains no \rightarrow -formulae and contains no \triangleright -formulae in its succedent, then no rule at all is applicable to s and so s is refutable as already shown in the proof of Thm. 3.12.

Base case $k = 1$: if s obeys the \ddagger conditions and the proof-search involves at most one application of the transitional rules in any branch, then each premise instance of s leads upwards to at least one non-derivable leaf sequent to which no rule is applicable. This leaf is again refutable as shown in the proof of Theorem 3.12. The Inversion Lemmas then allow us to conclude that the premise instance itself is refutable since all rule applications in this branch must be static rules. Thus each premise instance π_i of s under the transitional rules is refutable in some world w_i in some model M_i . Let w_0 be a new world and put $w_0 R w_i$ for every w_i and put $w_0 R w$ for each w which is an R_i^- -successor of any w_i in any model M_i , and put $w_0 \in \vartheta(p)$ iff p is in the antecedent of s . The new world w_0 makes every atomic formula in the antecedent of s true and makes every atomic formula in the succedent of s false. There are no conjunctions or disjunctions or \rightarrow -formulae in s . Every $\varphi \rightarrow \psi$ in the antecedent of s appears in the antecedent

of every premise instance π_i as $\varphi \rightarrow \psi$, so each w_i makes $\varphi \rightarrow \psi$ true, and hence w_0 makes $\varphi \rightarrow \psi$ true. Every $\triangleright\psi$ in the antecedent of s appears in the antecedent of every premise instance π_i and so does ψ , so each w_i makes ψ true, and hence w_0 makes $\triangleright\psi$ true. For every \multimap -formula $\varphi \multimap \psi$ in the succedent of s , the premise instance π_i corresponding to a $\rightarrow R$ -rule application with $\varphi \multimap \psi$ as the principal formula will contain φ in its antecedent and contain ψ in its succedent. The corresponding world w_i will make φ true and make ψ false, meaning that w_0 will falsify $\varphi \multimap \psi$. Similarly, for every \triangleright -formula $\triangleright\psi$ in the succedent of s , the world w_j obtained from a $\triangleright R$ -rule application with $\triangleright\psi$ as the principal formula will falsify ψ , meaning that w_0 will falsify $\triangleright\psi$. Thus w_0 will refute s as claimed.

Induction case $k + 1$ for $k > 0$: The induction hypothesis is that the lemma holds for all sequents s that obey the \ddagger -conditions and whose proof-search involves at most k applications of the transitional rules in any branch.

Now suppose that s obeys the \ddagger -conditions and the backward proof search for s contains $k + 1$ applications of the transitional rules. Consider the bottom-most application of the transitional rules (if any) along any branch ending at a premise instance π of s . Suppose the conclusion sequent of this bottom-most application is c . This application falls under the induction hypothesis and so c must be falsifiable in some model. The rules between c and π are all static rules, if any, and so are semantically invertible, meaning that the sequent π must be falsifiable in some model. Thus each premise instance π_i of s under the transitional rules is refutable in some world w_i in some model M_i . The same construction as in the base case for $k = 1$ suffices to deliver a model and a world that refutes s as claimed.

Corollary 4.3. *If the end-sequent $\Gamma_0 \vdash \Delta_0$ is not derivable using backward proof search according to our strategy then $\Gamma_0 \vdash \Delta_0$ is refutable.*

Corollary 4.4. *If φ_0 is KM-valid then $\vdash \varphi_0$ is SKM-derivable.*

As for KM_{lin} , our proofs yield the finite model property for KM as an immediate consequence, although for KM this is already known [25].

5 Related Work

Ferrari et al [14] give sequent calculi for intuitionistic logic using a compartment Θ in the antecedents of their sequents $\Theta; \Gamma \vdash \Delta$. This compartment contains formulae that are not necessarily true now, but are true in all strict successors. Fiorino [15] gives a sequent calculus using this compartment for LC. This yields linear depth derivations, albeit requiring a semantic check which is quadratic. Both [14,15] build in aspects of Gödel-Löb logic by allowing (sub)formulae to cross from the succedent of the conclusion into the compartment Θ . Our calculus differs by giving syntactic analogues \triangleright and \multimap for these meta-level features, and by requiring no compartments, but it should be possible to adapt these authors' work to design sequent calculi for KM_{lin} with linear depth derivations.

Restall [28] investigates “subintuitionistic logics” where each of the conditions on Kripke frames of reflexivity, transitivity and persistence can be dropped. The logic of our novel connective \Rightarrow can be seen as the logic bka , which lacks reflexivity, but has the additional conditions of linearity and converse well-foundedness, which Restall does not consider. The models studied by Restall all require a root world, and thus they disallow sequences $\cdots x_3 R x_2 R x_1$ which are permitted by KM_{lin} -models. Ishigaki and Kikuchi [19] give “tree-sequent” calculi for the first-order versions of some of these subintuitionistic logics. Thus “tree-sequent” calculi for KM and KM_{lin} are possible, but our calculi require no labels.

Labelled sequent calculi for KM and KM_{lin} are possible by extending the work of Dyckhoff and Negri [13] but termination proofs and complexity results for labelled calculi are significantly harder than our proofs.

Garg et al [16] give labelled sequent calculi for intuitionistic modal logics and general conditions on decidability. Their method relies on a first-order characterisation of the underlying Kripke relations, but converse well-foundedness is not first-order definable. Labelled calculi can handle converse well-founded frames by allowing formulae to “cross” sides as in our calculus, but it is not clear whether the method of Garg et al [16] then applies.

Our complexity results follow directly from our calculi; a possible alternative may be to adapt the polynomial encoding of LC into classical satisfiability [8].

6 Conclusion

We have seen that the internal *propositional* logic of the topos of trees is KM_{lin} . Indeed it may be tempting to think that KM_{lin} is just LC , as both are sound and complete with respect to the class of finite sequences of reflexive points, but note that we cannot express the modality \triangleright in terms of the connectives of LC .

Linear frames seem concordant with the *step-indexing* applications of later, based as they are on induction on the natural numbers rather than any branching structure, but seem less natural from a *types* point of view, which tend to build on intuitionistic logic. For a possible type-theoretic interpretation of linearity see Hirai’s λ -calculus for LC with applications to ‘waitfree’ computation [17]. More broadly our work provides a proof-theoretical basis for future research into computational aspects of intuitionistic Gödel-Löb provability logic.

The topos of trees, which generalises some previous models, has itself been generalised as a model of guarded recursion in several ways [4,3,24]. These categories do not all correspond to KM_{lin} ; some clearly fail to be linear. The logical content of these general settings may also be worthy of study.

The most immediate application of our proof search algorithm may be to provide automation for program logics that use later [18,2,9]. Support for a richer class of connectives, such as first and higher order quantifiers, would be desirable. We in particular note the ‘backwards looking box’ used by Bizjak and Birkedal [6] in sheaves over the first uncountable ordinal ω_1 , and subsequently in the topos of trees by Clouston et al [9] to reason about coinductive types.

Acknowledgments We gratefully acknowledge helpful discussions with Lars Birkedal, Stephané Demri, Tadeusz Litak, and Jimmy Thomson, and the comments of the reviewers of this and a previous unsuccessful submission.

References

1. Appel, A.W., Melliès, P.A., Richards, C.D., Vouillon, J.: A very modal model of a modern, major, general type system. In: POPL. pp. 109–122 (2007)
2. Bengtson, J., Jensen, J.B., Sieczkowski, F., Birkedal, L.: Verifying object-oriented programs with higher-order separation logic in Coq. In: ITP, pp. 22–38 (2011)
3. Birkedal, L., Møgelberg, R.E.: Intensional type theory with guarded recursive types qua fixed points on universes. In: LICS. pp. 213–222 (2013)
4. Birkedal, L., Møgelberg, R.E., Schwinghammer, J., Støvring, K.: First steps in synthetic guarded domain theory: step-indexing in the topos of trees. LMCS 8(4) (2012)
5. Birkedal, L., Schwinghammer, J., Støvring, K.: A metric model of lambda calculus with guarded recursion. In: FICS. pp. 19–25 (2010)
6. Bizjak, A., Birkedal, L., Miculan, M.: A model of countable nondeterminism in guarded type theory. In: RTA-TLCA. pp. 108–123 (2014)
7. Boolos, G.: The logic of provability. CUP (1995)
8. Chagrov, A., Zakharyashev, M.: Modal Logic. OUP (1997)
9. Clouston, R., Bizjak, A., Grathwohl, H.B., Birkedal, L.: Programming and reasoning with guarded recursion for coinductive types. In: FoSSaCS (2015)
10. Coquand, T.: Infinite objects in type theory. In: TYPES. pp. 62–78 (1993)
11. Corsi, G.: Semantic trees for Dummett’s logic LC. Stud. Log. 45(2), 199–206 (1986)
12. Dreyer, D., Ahmed, A., Birkedal, L.: Logical step-indexed logical relations. In: LICS. pp. 71–80 (2009)
13. Dyckhoff, R., Negri, S.: Proof analysis in intermediate logics. Arch. Math. Log. 51(1-2), 71–92 (2012)
14. Ferrari, M., Fiorentini, C., Fiorino, G.: Contraction-free linear depth sequent calculi for intuitionistic propositional logic with the subformula property and minimal depth counter-models. J. Autom. Reason. 51(2), 129–149 (2013)
15. Fiorino, G.: Terminating calculi for propositional Dummett logic with subformula property. J. Autom. Reason. 52(1), 67–97 (2014)
16. Garg, D., Genovese, V., Negri, S.: Countermodels from sequent calculi in multi-modal logics. In: LICS. pp. 315–324 (2012)
17. Hirai, Y.: A lambda calculus for Gödel–Dummett logic capturing waitfreedom. In: FLOPS, pp. 151–165 (2012)
18. Hobor, A., Appel, A.W., Nardelli, F.Z.: Oracle semantics for concurrent separation logic. In: ESOP, pp. 353–367 (2008)
19. Ishigaki, R., Kikuchi, K.: Tree-sequent methods for subintuitionistic predicate logics. In: TABLEAUX. pp. 149–164 (2007)
20. Krishnaswami, N.R., Benton, N.: A semantic model for graphical user interfaces. In: ICFP. pp. 45–57 (2011)
21. Krishnaswami, N.R., Benton, N.: Ultrametric semantics of reactive programs. In: LICS. pp. 257–266 (2011)
22. Litak, T.: A typing system for the modalized Heyting calculus. In: COS (2013)
23. Litak, T.: Constructive modalities with provability smack, author’s cut v. 2.03 (2014), retrieved from author’s website.

- 24. Milius, S., Litak, T.: Guard your daggers and traces: On the equational properties of guarded (co-) recursion. arXiv:1309.0895 (2013)
- 25. Muravitsky, A.: Logic KM: A biography. *Outstanding Contributions to Logic* 4, 155–185 (2014)
- 26. Nakano, H.: A modality for recursion. In: *LICS*. pp. 255–266 (2000)
- 27. Pottier, F.: A typed store-passing translation for general references. In: *POPL*. pp. 147–158 (2011)
- 28. Restall, G.: Subintuitionistic logics. *NDJFL* 34(1), 116–129 (1994)
- 29. Rowe, R.N.: *Semantic Types for Class-based Objects*. Ph.D. thesis, Imperial College London (2012)
- 30. Sonobe, O.: A Gentzen-type formulation of some intermediate propositional logics. *J. Tsuda College* 7, 7–14 (1975)
- 31. Troelstra, A., Schwichtenberg, H.: *Basic Proof Theory*. CUP (1996)
- 32. Wolter, F., Zakharyashev, M.: Intuitionistic modal logics. In: *Logic and Foundations of Mathematics*, pp. 227–238 (1999)